INFORMATION AND CONTROL 30, 86–95 (1976)

On Permutation–Reset Automata

ELMAR DILGER

Institute for Information Sciences, University of Tübingen, Germany

A series decomposition of permutation–reset automata is set up. The structure of the characteristic semigroups of its components is determined as factor groups and constituents of the group of the original automaton. It is shown that a realization of this decomposition contains fewer components than in the usual Krohn–Rhodes decomposition of permutation–reset automata.

1. INTRODUCTION

In the usual decomposition theories of automata, permutation–reset automata are not decomposed directly but are first covered by grouplike and identity–reset automata (Ginzburg, 1968; Arbib, 1969). The grouplike automata are then decomposed by the well-known group theoretical theorem of Jordan–Hölder into grouplike automata with simple groups. Zeiger (1968) gave a method to cover a permutation automaton by a cascade of permutation automata in which one of the components has the same state set as the original automaton.

We present a decomposition in which the state sets as well as the semigroups of the components are small compared to those of the original automaton. The irreducible components of such a decomposition of permutation automata are, in general, no longer grouplike automata with simple groups, but are permutation automata with so-called primitive groups. Nevertheless these irreducible permutation–reset automata can then be covered by grouplike automata with simple groups and flip-flops. However, the number of components needed to decompose an automaton in this way is, in general, considerably smaller than in the classical decomposition.

In Section 2 we treat permutation automata and in Section 3 we extend the results to permutation–reset automata.

In addition to the familiar results of structure theory of automata (Hartmanis and Stearns, 1966; Ginzburg, 1968; Arbib, 1969). we need the following permutation-group theoretical notions:

Copyright © 1976 by Academic Press, Inc.
All rights of reproduction in any form reserved.

(i) We say a group G acts on a set Q, if each $g \in G$ induces a mapping $Q \to Q$, $q \to q^g$, such that $q^1 = q$ and $q^{(g_1 g_2)} = (q^{g_1})^{g_2}$ for all $q \in Q$ and $g_1, g_2 \in G$. If $1 \in G$ is the only element x from G with $q^x = q$ for all $q \in Q$, we call G a permutation group on Q (in short, $G \leqslant \mathrm{Sym}_Q$).

(ii) A group G acts transitively on Q, if for all $q_1, q_2 \in Q$ there is a $g \in G$ such that $q_1{}^g = q_2$.

(iii) A permutation group G is said to be primitive on Q, if it is transitive on Q and if there exists no $B \subseteq Q$, $|B| > 1$, $B \neq Q$ such that for all $g \in G$:

$$B \cap B^g \in \{B, \varnothing\} \qquad (\text{where } B^g = \{q^g \mid q \in B\}).$$

(iv) If $\varnothing \neq B \subseteq Q$, G is a permutation group on Q, H is the subgroup of G which fixes B, and H_B is the subgroup of G which fixes each point of B, then we call the group H/H_B (considered as a permutation group on B) a constituent of G.

2. The Main Theorem for Permutation Automata

In this section, only automata that have groups as characteristic semigroups are considered. For infinite automata, the definition of permutation automata is slightly modified in order to obtain groups in this case too.

Definition 1. An automaton $A = (X, Y, Q, \delta, \lambda)$, where $\delta: X \times Q \to Q$, $\lambda: X \times Q \to Y$, is said to be a permutation automaton, if for all $x \in X$ there are $w, w' \in X^*$ (the free semigroup generated by X) such that for all $q \in Q$: $\delta(xw, q) = q$ and $\delta(w'x, q) = q$. (If Q is finite, an equivalent definition is: the mapping $q \to \delta(x, q)$ is a permutation of Q for all $x \in X$.)

We proof the following

Theorem 1. *If $A = (X, Y, Q, \delta, \lambda)$ is a connected permutation automaton which possesses a nontrivial closed partition, then A is isomorphic to a series connection $M_1 \textcircled{\ominus} M_2$, where the semigroup of M_1 is a group isomorphic to a factor group of the group of A and the semigroup of M_2 is a group isomorphic to a constituent of the group of A. Both M_1 and M_2 are connected permutation automata.*

In what follows, $A = (X, Y, Q, \delta, \lambda)$ designs a permutation automaton that is connected and that possesses a nontrivial closed partition π (i.e., a partition with substitution property), which means: The group G of A is transitive but not promitive on Q.

Lemma 1 is proved in Wielandt (1964) only for finite groups, but one can easily show that it also remains valid for infinite groups.

LEMMA 1 (Wielandt (1964), Proposition 7.2). *Let $\bar{Q} = \{B_1, \ldots, B_k\}$ be a complete nontrivial block system of the imprimitive group G, and let $\bar{g}$ be the permutation on $\bar{Q}$ induced by g,*

$$\bar{g} = \begin{pmatrix} B_1 & \cdots & B_k \\ (B_1)^g & \cdots & (B_k)^g \end{pmatrix}.$$

Then the maps $\bar{g}$ form a permutation group $\bar{G}$ on $\bar{Q}$ and the mapping $g \to \bar{g}$ is a homomorphism of G onto $\bar{G}$. The kernel N of this homomorphism consists of those permutations of G that take each of the blocks B_i $(i = 1, \ldots, k)$ into itself. $\bar{G}$ is transitive on $\bar{Q}$. The blocks B_i are fixed sets but not necessarily orbits of N.

Therefore, we know that G acts transitively on the set of blocks of π and there is a homomorphism from G into $\mathrm{Sym}_{\{B_1, B_2, \ldots\}}$; the kernel N of this homomorphism consists of those permutations of G which take each of the blocks into itself.

Furthermore, there exists a series decomposition $M_1 \textcircled{\scriptsize :} M_2$ of A (one must choose a second partition τ with blocks $\{C_j\}$ such that $\pi\tau = 0$) with

$$\begin{aligned} &M_1 = (X, \{B_i\} \times X, \{B_i\}, \delta_\pi, e) \\ &\text{where } \delta_\pi(x, B_r) = B_k \Leftrightarrow \forall q \in B_r\colon \delta(x, q) \in B_k \\ &\text{and } e \text{ is the identity map,} \end{aligned}$$

and

$$\begin{aligned} &M_2 = (\{B_i\} \times X, Y, \{C_j\}, \delta_2, \lambda_2) \\ &\text{where } \delta_2(C_j, (B_i, x)) = C_k \Leftrightarrow \delta(C_j \cap B_i, x) \in C_k \\ &\text{and } \lambda_2(C_j, (B_i, x)) = \lambda(C_j \cap B_i, x) \end{aligned}$$

(Hartmanis and Stearns, 1966).

From Lemma 1, we know that the semigroup of M_1 is a group isomorphic to G/N and is transitive on the blocks of π. Thus, M_1 is a connected permutation automaton with group G/N. Now we look for a suitable second partition τ of the state set in order to characterize the semigroup of M_2.

DEFINITION 2. Let $B_1 = \{b_1, b_2, \ldots\}$ be a block of π, and $H = \{g \in G \mid B_1{}^g = B_1\}$. H is a subgroup of G. If $R = \{r_1, r_2, \ldots\}$ is a system of coset representatives of $G : H$ (that is $G = \bigcup_{r_i \in R} Hr_i$ and $Hr_i \cap Hr_j = \varnothing$ if $r_i \neq r_j$) we have

$$Q = \bigcup_{r_i \in R} B_1^{r_i} \qquad \text{and} \qquad B_1^{r_i} \cap B_1^{r_j} = \varnothing \qquad \text{if} \quad r_i \neq r_j.$$

As blocks of the second partition τ we define now the sets $C_j = \{b_j^{r_k} \mid r_k \in R\}$. Without loss of generality we set $r_1 = 1$. If we define $B_j = B_1^{r_j}$ we have $C_i \cap B_j = \{b_i^{r_j}\}$ and this implies $\pi\tau = 0$.

LEMMA 2. *Under the assumptions of Theorem* 1 *we have*: *H acts transitively on B_1.*

Proof. Let $b_1, b_2 \in B_1$. G is transitive on Q; therefore, there is a $g \in G$ with $b_1^g = b_2$. Now $b_1^g \in B_1^g \cap B_1 \neq \varnothing$; B_1 and B_1^g are blocks of a closed partition and thus $B_1 = B_1^g$ and this means $g \in H$.

Now we consider relations between the semigroup of M_2 and the group H. To do this, let us look at the input semigroup of M_2.

DEFINITION 3. Define $FS(B_i, X)$ to be the free semigroup generated by $\{B_i \mid i = 1, 2,...\} \times X$ and let $H_{B_1} = \{h \in H \mid b^h = b \; \forall b \in B_1\}$. Then H_{B_1} is a normal subgroup of H. Since for all $x \in X$ and $r_i \in R$ there is exactly one $h \in H$ and exactly one $r_j \in R$ such that $r_i x = h r_j$, we always have $1 = |\, r_i x R^{-1} \cap H \,|$ (we interprete $x \in X$ to be a generating element of G too) and thus we can define the following map

$$\phi: \{B_i \mid i = 1, 2,...\} \times X \to H/H_{B_1}$$
$$(B_i, x) \to (r_i x R^{-1} \cap H) H_{B_1}$$

where $r_i x R^{-1}$ means $\{r_i x r_j^{-1} \mid r_j \in R\}$.

It is well known that for free algebras (cf. Grätzer, 1968, Sect. 24), ϕ can be extended into a homomorphism and there exists a congruence relation θ such that

$$FS(B_i, X)/\theta \text{ is isomorphic to a subsemigroup of } H/H_{B_1}.$$

Thus, we have

LEMMA 3. *The mapping ϕ extends to a homomorphism ϕ such that $\phi(FS(B_i, X))$ is isomorphic to a subsemigroup of H/H_{B_1}.*

However we can say more:

LEMMA 4. *$\phi(FS(B_i, X))$ is isomorphic to H/H_{B_1}.*

Proof. To show that ϕ is surjective, it is enough to show that the homomorphism induced by

$$\psi: \{B_i \mid i = 1, 2,...\} \times X \to H$$
$$(B_i, x) \to r_i x R^{-1} \cap H$$

is surjective.

Let $h \in H$; then there exist $x_1, x_2, \ldots, x_n \in X$: $h = x_1 x_2 \cdots x_n$. For all $i \in \{1, 2, \ldots, n\}$, there exists exactly one $r_{ji} \in R$:

$$x_1 x_2 \cdots x_i r_{ji}^{-1} \in H$$

and, because $h \in H$, we have $r_{jn} = 1$. Therefore,

$$h = (x_1 r_{j1}^{-1})(r_{j1} x_2 r_{j2}^{-1}) \cdots (r_{j(n-1)} x_n r_{jn}^{-1}).$$

As for $i = 1, 2, \ldots, n-1$, $u_i = x_1 x_2 \cdots x_i r_{ji}^{-1} \in H$, and $u_i^{-1} u_{i+1} = r_{ji} x_{i+1} r_{j(i+1)}^{-1} \in H$, we have

$$r_{ji} x_{i+1} r_{j(i+1)}^{-1} = \psi(B_{ji}, x_{i+1})$$

and

$$x_1 r_{j1}^{-1} = \psi(B_1, x_1).$$

Thus, $h = \psi((B_1, x_1)(B_{j1}, x_2) \cdots (B_{j(n-1)}, x_n))$ and ψ is shown to be surjective.

Therefore, $FS(B_i, X)/\theta$ is isomorphic to H/H_{B_1} and, in particular, $FS(B_i, X)/\theta$ is a group.

Now we are able to fill the last remaining gap in the proof of Theorem 1.

LEMMA 5. *M_2 is a connected permutation automaton; the semigroup of M_2 is a group isomorphic to H/H_{B_1}.*

Proof. We consider the semigroup of M_2. It is $FS(B_i, X)/\simeq$ where "$\simeq$" denotes the following congruence relation:

$$w \simeq w' \Leftrightarrow \delta_2(C_k, w) = \delta_2(C_k, w')\ \forall C_k \qquad (w, w' \in FS(B_i, X)).$$

Now

$$\begin{aligned} & (B_i, x_1) \simeq (B_j, x_2) \\ \Leftrightarrow\ & \delta_2(C_k, (B_i, x_1)) = \delta_2(C_k, (B_j, x_2)) && \forall C_k \\ \Leftrightarrow\ & [(C_k \cap B_i)^{x_1}]_\tau = [(C_k \cap B_j)^{x_2}]_\tau && \forall C_k \\ \Leftrightarrow\ & [b_k^{r_i x_1}]_\tau = [b_k^{r_j x_2}]_\tau && \forall b_k \in B_1. \end{aligned}$$

From the construction of ϕ we know that there are $r_l, r_m \in R$:

$$r_i x_1 r_l^{-1} H_{B_1} = \phi(B_i, x_1)$$

and

$$r_j x_2 r_m^{-1} H_{B_1} = \phi(B_j, x_2).$$

If $g, \bar{g} \in G$ have the unique decompositions $g = hr_q$, $\bar{g} = \bar{h}r_p$ $(h, \bar{h} \in H, r_q, r_p \in R)$ then

$$[b_s{}^g]_\tau = [b_t{}^{\bar{g}}]_\tau \Leftrightarrow b_s{}^h = b_t{}^{\bar{h}}.$$

Thus it follows that

$$\begin{aligned}
&[b_k^{r_i x_1}]_\tau = [b_k^{r_j x_2}]_\tau && \forall b_k \in B_1 \\
\Leftrightarrow\ &[b_k^{\phi(B_i, x_1) r_l}]_\tau = [b_k^{\phi(B_j, x_2) r_n}]_\tau && \forall b_k \in B_1 \\
\Leftrightarrow\ &b_k^{\phi(B_i, x_1)} = b_k^{\phi(B_j, x_2)} && \forall b_k \in B_1 \\
\Leftrightarrow\ &\phi(B_i, x_1) = \phi(B_j, x_2) \\
\Leftrightarrow\ &((B_i, x_1), (B_j, x_2)) \in \theta.
\end{aligned}$$

For words of length greater than one this can be shown in a similar way.

Thus, we have that the relations θ and $\simeq$ are identical and the semigroup of M_2 is a group isomorphic to H/H_{B_1}. From Lemma 2, we know that H acts transitively on B_1; from Lemma 4, we know that the map ψ is surjective. Between the actions of $FS(B_i, X)$ and H the following relation holds:

$$\delta_2(C_j, (B_i, x)) = C_k \Leftrightarrow b_j^{\psi(B_i, x)} = b_k.$$

Therefore, the semigroup of M_2 is transitive, i.e., M_2 is also a connected permutation automaton that proves Theorem 1.

We can obtain still deeper insight into the structure of the group G of A if we consider the wreath product of the group of M_2 with the group of M_1.

DEFINITION 4 (Huppert (1967), Chap. I, 15, 1). If L is a permutation group on a set Q and K is a group, then the wreath product $K \sim L$ is the group

$$\{(f, l) \mid f \text{ is a map from } Q \text{ to } K,\ l \in L\}$$

with multiplication $(f_1, l_1)(f_2, l_2) = (g, l_1 l_2)$, where $g(q) = f_1(q) f_2(q^{l_1})$ $\forall q \in Q$.

THEOREM 2. *The group G of A is isomorphic to a subgroup of $H/H_{B_1} \sim G/N$.*

Proof. (a) The map $\zeta: G \to H/H_{B_1} \sim G/N$

$$g \to (f_g, gN),$$

with

$$f_g\colon \{B_i\} \to H/H_{B_1}$$

$$B_i = B_1^{r_i} \to (r_i g R^{-1} \cap H)\, H_{B_1}$$

is a homomorphism.

We have

$$\zeta(g_1)\,\zeta(g_2) = (f_{g_1}, g_1N)(f_{g_2}, g_2N) = (\hat{f}, g_1g_2N),$$

where

$$\begin{aligned}
\hat{f}(B_i) &= f_{g_1}(B_i)\, f_{g_2}(B_i^{g_1N}) \\
&= (r_i g_1 R^{-1} \cap H)\, H_{B_1} (r_j g_2 R^{-1} \cap H)\, H_{B_1} \\
&\quad \text{(with } r_i g_1 = h r_j\,,\ h \in H\text{)} \\
&= h H_{B_1} (r_j g_2 R^{-1} \cap H)\, H_{B_1} \\
&\quad \text{(with } r_j g_2 = \bar{h} r_s\,,\ \bar{h} \in H\text{)} \\
&= h H_{B_1} \bar{h} H_{B_1} = h\bar{h} H_{B_1} = (r_i g_1 r_j^{-1})(r_j g_2 r_s^{-1})\, H_{B_1} \\
&= r_i g_1 g_2 r_s^{-1} H_{B_1} = (r_i g_1 g_2 R^{-1} \cap H)\, H_{B_1} = f_{g_1g_2}(B_i).
\end{aligned}$$

Therefore, $\zeta(g_1)\,\zeta(g_2) = \zeta(g_1g_2)$.

(b) ζ is injective. Let $\zeta(g) = 1\ (\in H/H_{B_1} \sim G/N)$, i.e., $\zeta(g) = (f_0, N)$, where $f_0\colon B_i \to H_{B_1}\ \forall B_i$. Then (i) $gN = N$, which means $g \in N$ and (ii) $r_i g R^{-1} \cap H \subseteq H_{B_1}\ \forall r_i \in R$. Since N is a subgroup of H and N is a normal subgroup of G, we know from (i) that $r_i g r_i^{-1} \in H\ \forall r_i \in R$. From (ii) we get $r_i g r_i^{-1} \in H_{B_1}\ \forall r_i \in R$ and this implies that $g \in \bigcap_{r_i \in R} r_i^{-1} H_{B_1} r_i = 1$. Thus, ζ is injective.

3. Permutation–Reset Automata

We extend our results to permutation–reset automata. We shall consider those permutation–reset automata for which the group G generated by the permutation inputs acts transitively on Q. Since for resets, every partition is closed, we get Theorem 3 at once as a corollary of Theorem 1.

THEOREM 3. *If $A = (X, Y, Q, \delta, \lambda)$ is a permutation–reset automaton that is connected under the permutation inputs and that possesses a nontrivial closed partition, then A is isomorphic to a series connection $M_1 \textcircled{\scriptsize S} M_2$. M_1 and M_2 are permutation–reset automata that are connected under their permutation inputs. The group generated by the permutation inputs of M_1 is isomorphic to a factor group of G (the group generated by the permutation inputs of A) and the group generated by the permutation inputs of M_2 is isomorphic to a constituent of G.*

For a proof and related material see Dilger (1975).

4. EXAMPLE

As an example we consider the automaton $A = (X, Y, Q, \delta, \lambda)$ with $X = \{x, y\}$, $Y = \{a, b\}$, $Q = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$; δ and λ are described by Table I. A is a connected permutation automaton and has the closed partition $\pi = \{[1, 2, 3], [4, 5, 6], [7, 8, 9]\}$.

TABLE I

A	x	y
1	2/a	4/a
2	3/a	6/a
3	1/b	5/a
4	7/b	8/a
5	9/b	7/a
6	8/a	9/a
7	5/b	1/b
8	6/a	3/b
9	4/b	2/b

If we set $B_1 = [1, 2, 3]$, $B_2 = [4, 5, 6]$, $B_3 = [7, 8, 9]$, then $B_1{}^y = B_2$ and $B_1{}^{yx} = B_3$. Thus, we can choose $r_1 = 1$, $r_2 = y$, $r_3 = yx$. For M_1 we obtain the results in Table II.

TABLE II

M_1	x	y
B_1	$B_1/(B_1, x)$	$B_2/(B_1, y)$
B_2	$B_3/(B_2, x)$	$B_3/(B_2, y)$
B_3	$B_2/(B_3, x)$	$B_1/(B_3, y)$

The group of M_1 is $\mathrm{Sym}_{\{B_1,B_2,B_3\}} = S_3$. We choose as blocks of the second partition

$$C_1 = [1, 1^y, 1^{yx}] = [1, 4, 7],$$
$$C_2 = [2, 2^y, 2^{yx}] = [2, 6, 8],$$
$$C_3 = [3, 3^y, 3^{yx}] = [3, 5, 9].$$

Then we obtain for M_2 the results given in Table III. The group of M_2 is again $\mathrm{Sym}_{\{C_1,C_2,C_3\}} = S_3$.

TABLE III

M_2	(B_1, x)	(B_2, x)	(B_3, x)	(B_1, y)	(B_2, y)	(B_3, y)
C_1	C_2/a	C_1/b	C_3/b	C_1/a	C_2/a	C_1/b
C_2	C_3/a	C_2/a	C_2/a	C_2/a	C_3/a	C_3/b
C_3	C_1/b	C_3/b	C_1/b	C_3/a	C_1/a	C_2/a

The group S_3 is primitive on a set with three elements; therefore, M_1 and M_2 cannot be decomposed by our procedure. But according to Arbib (1969), we can simulate M_1 and M_2 by grouplike automata and then we can decompose these. If we do this, we obtain a simulation of A by grouplike automata with simple groups.

We need two grouplike automata with cyclic group of order 2
and two grouplike automata with cyclic group of order 3.

If we simulate A itself by a grouplike automaton, we must consider the group G of A. It can be shown that G is isomorphic to $S_3 \sim S_3$, so G is solvable and has order 1296. In that case we need for a decomposition of this grouplike automaton by grouplike automata with simple groups

four grouplike automata with cyclic group of order 2
and four grouplike automata with cyclic group of order 3.

Thus, in accordance with Theorem 2, in general, we do not need all the factors from a composition series of G to simulate A by our procedure.

ACKNOWLEDGMENTS

The author thanks Professor M. Dal Cin for many helpful discussions and suggestions, Professor W. Güttinger for the hospitality of his institute, and Professor H. Wielandt for his support.

RECEIVED: February 21, 1975; REVISED: June 13, 1975

References

ARBIB, M. A. (1969), "Theories of Abstract Automata," Prentice-Hall, Englewood Cliffs, N.J.

DILGER, E. (1975), Zur Strukturtheorie abstrakter Automaten, thesis, University of Tübingen.

GINZBURG, A. (1968), "Algebraic Theory of Automata," Academic Press, New York/London.

GRÄTZER, G. (1968), "Universal Algebra," Van Nostrand, Princeton, N.J.

HARTMANIS, J. AND STEARNS, R. E. (1966), "Algebraic Structure Theory of Sequential Machines," Prentice-Hall, Englewood Cliffs, N.J.

HUPPERT, B. (1967), "Endliche Gruppen I," Springer, Berlin/Heidelberg.

WIELANDT, H. (1964), "Finite Permutation Groups," Academic Press, New York/London.

ZEIGER, H. P. (1968), Cascade decomposition of automata using covers, *in* "Algebraic Theory of Machines, Languages, and Semigroups" (M. A. Arbib, Ed.), pp. 55–80, Academic Press, New York/London.